امین رای

گسترش فناوری پارس امین رای

نـام سنـد لیست تهدیدهای احتمالی شناسایی شده برای سیستم سادا	
تهیه کننده: گسترش فناوری پارس امین رای **طبقه بندي:** محرمانه	**تاریخ نشـر:** ۱۴۰۲/۰۴/۱۷
کد سند: AMR_SADA_Potential_Threats_14020417_v1.0	**تاریخ آخرین بازنگري:** ۱۴۰۲/۰۵/۲۱

به‌نام خدا

فهرست مطالب

عنوان	صفحه
فصل ۱- مروری بر مدلسازی تهدیدها	**۴**
فصل ۲- تهدیدهای شناسایی شده	**۶**
۲-۱- مروری بر چارچوب STRIDE	۶
۲-۲- عاملین تهدید در سیستم سادا	۷
۲-۳- اهداف احتمالی مهاجمین در سیستم سادا	۷
۲-۴- آسیب‌پذیری‌های احتمالی سیستم سادا	۸
۲-۵- فهرست تهدیدهای احتمالی	۱۰

فصل ۱- مروری بر مدلسازی تهدیدها

یکی از مهمترین فعالیت‌هایی که در چرخه حیات توسعه امن نرم‌افزارها باید انجام گیرد، مدلسازی تهدید است. مدلسازی تهدید، یک فرایند تکرارپذیر برای شناسایی، ارزیابی و کاهش تهدیدهای فنی و کسب‌وکاری یک سیستم یا یک مولفه است. این فعالیت بهتر است به عنوان بخشی از فاز طراحی نرم‌افزار انجام گیرد، اما اجرای آن برای نرم‌افزارهای توسعه یافته نیز می‌تواند مفید باشد؛ زیرا امکان شناسایی انواع تست‌های امنیتی ضروری و محل اجرای آنها را برای نرم‌افزار فراهم می‌کند. علاوه بر این، دلیل ریشه‌ای برخی از آسیب‌پذیری‌های شناسایی شده در فازهای بعدی نیز در این فعالیت قابل شناسایی خواهند بود.

مدلسازی تهدید، بهتر است با مشارکت همه ذینفعان سیستم اعم از کارشناسان ارشد طراحی و معماری، عملیات و زیرساخت، امنیت و دیگر کارشناسانی که به نوعی سیستم را از جنبه فنی و کسب‌وکاری به خوبی می‌شناسند، انجام شود. این فرایند، معمولا شامل ۶ گام زیر است:

۱. شناخت معماری سیستم برمبنای مستندات، دیاگرام‌ها و دیگر مصنوعات معماری
۲. شناسایی دارایی‌های حیاتی سیستم شامل داده‌ها و عملکردهای حیاتی آن
۳. تعیین کنترل‌های امنیتی به کار گرفته شده برای حفاظت از دارایی‌های حیاتی سیستم
۴. شناسایی تهدیدها و مستندسازی آنها
۵. رتبه‌بندی تهدیدها
۶. تعیین راهکارهای کاهش یا رفع تهدیدها

دیاگرام DFD، یکی از ابزارهای مفید برای مدلسازی سیستم است. این دیاگرام، محل پردازش و ذخیره‌سازی موقت و دائمی داده‌ها و همچنین جریان داده‌ها در سیستم را به خوبی نشان می‌دهد. علاوه بر این، موجودیت‌های خارجی که با سیستم در تعامل هستند نیز در این دیاگرام، قابل مشاهده هستند. با توجه به این ویژگی‌ها، در مدلسازی تهدید، معمولا از DFD برای ایجاد مدل تهدید سیستم استفاده می‌شود. این مدل را می‌توان در ابزارهای مدلسازی تهدید همانند Microsoft Threat Modeling Tool و OWASP Threat Dragon نیز ترسیم کرد.

پس از ترسیم DFD سیستم، برای شناسایی تهدیدها، می‌بایست مرزهای اعتماد (Trust Boundary) را در این نمودار مشخص کرد. در این مرزها که بین بخش‌های مختلف نمودار قرار خواهند گرفت، سطح trust تغییر می‌کند. به عنوان مثال، فایروال‌ها، محدوده فرایندها، محدوده ماشین، سیستم فایل و غیره، نمونه محل‌هایی در نمودار هستند که منجر به ایجاد یک مرز اعتماد می‌شوند.

شناسایی تهدیدها را می‌توان برمبنای چارچوب STRIDE و مراجعی همانند CAPEC، OWASP Automated Threats، OWASP Top 10 و دیگر مراجع معتبر انجام داد. علاوه بر این، شناسایی عاملین

تهدید، ترسیم درخت تهدیدها و الگوی حملات و توجه به اصول طراحی امن نیز در شناسایی تهدیدها می‌توانند مفید واقع شوند.

خروجی مدلسازی تهدید، دیاگرام‌ها و مستندات توصیف معماری و همچنین لیست تهدیدهای شناسایی شده به همراه راهکارهای رفع یا کاهش آنها است.

مستند پیش‌رو، لیست تهدیدهای احتمالی شناسایی شده برای سیستم سادا است که توسط شرکت «امین رای» تهیه شده است. دیاگرام DFD و مدل تهدید ترسیم شده برای این سامانه، در یک سند جداگانه ارائه شده است.

فصل ۲- تهدیدهای شناسایی شده

در فصل پیش‌رو فهرست تهدیدهای احتمالی که سیستم سادا با آنها مواجه است، آورده شده‌اند. این تهدیدها برمبنای بررسی‌های انجام شده روی معماری این سیستم و جلسات برگزار شده با کارشناسان سیستم و همچنین بررسی مستندات مربوطه، شناسایی شده‌اند.

تهدیدها برمبنای چارچوب STRIDE دسته‌بندی شده‌اند. به همین دلیل، این چارچوب و شش دسته آن در بخش ۲-۱، توصیف شده‌اند. سپس در بخش ۲-۲، عاملین تهدیدها[۱] در این سیستم معرفی شده‌اند. عاملین تهدید، افراد یا گروه‌هایی هستند که توانای بالفعل کردن یک تهدید بالقوه را دارند. اهداف مهاجمین از حمله به سیستم سادا برمبنای شناخت بدست آمده از این سیستم، در بخش ۲-۳، فهرست شده‌اند. با در نظر گرفتن این اهداف، می‌توان تهدیدهای احتمالی سیستم را شناسایی کرد. سپس فهرست برخی از آسیب‌پذیری‌های احتمالی در سیستم سادا که می‌توانند در بالفعل شدن تهدیدها توسط عاملین تهدید، مورد بهره‌برداری قرار گیرند، در بخش ۲-۴آورده شده‌اند. در نهایت برمبنای تمام این موارد، فهرست تهدیدهای احتمالی، تاثیر آنها بر سیستم و راهکارهای رفع یا کاهش اثر این تهدیدها، در بخش ۲-۵ تشریح شده‌اند.

۲-۱- مروری بر چارچوب STRIDE

با توجه به اینکه تهدیدهای شناسایی شده برمبنای چارچوب STRIDE دسته‌بندی شده‌اند، در این بخش به معرفی این چارچوب پرداخته شده است.

- **Spoofing:** این دسته از تهدیدها با هدف دسترسی به اطلاعات هویتی و شناسایی موجودیت‌ها و سوءاستفاده از آنها انجام می‌شود. در این صورت، ویژگی اصالت[۲]، از مجموعه ویژگی‌های مهم در امنیت اطلاعات، تامین نخواهد شد.
- **Tampering:** در این دسته از تهدیدات، مهاجم سعی می‌کند داده‌ها و دیگر آرتیفکت‌ها را به طور غیرمجاز تغییر دهد و به عبارت بهتر، آنها را دستکاری کند. این داده‌ها ممکن است داده‌های ذخیره شده و یا داده‌های در حال انتقال باشند. در این حالت، اصل صحت[۳] داده‌ها که یکی از اصول مهم در امنیت اطلاعات است، نقض خواهد شد.
- **Repudiation:** این دسته از تهدیدات، با هدف دور زدن ویژگی انکارناپذیری از امنیت اطلاعات، انجام می‌شوند و در آن کاربر، فعالیتی را که انجام داده است، انکار می‌کند و سیستم توانایی ثابت کردن انجام آن فعالیت توسط آن کاربر و به عبارت بهتر ردیابی فعالیتهای او را ندارد.

---

[۱] Threat Agent or Threat Actor

[۲] Authenticity

[۳] Integrity

- **Information Disclosure**: در این نوع از تهدیدها، هدف مهاجم دستیابی غیرمجاز به داده‌ها و اطلاعات ذخیره شده یا در حال انتقال است. در این حالت، اصل محرمانگی از امنیت اطلاعات، نقض خواهد شد.
- **Denial of Service**: هدف مهاجم در این تهدید، از دسترس خارج کردن منابع موردنیاز برای کاربران قانونی آنها است. این منابع، ممکن است منابع پردازشی، ذخیره‌سازی و شبکه‌ای باشند. در واقع در این تهدید اصل دسترس‌پذیری در امنیت، نقض خواهد شد.
- **Elevation of Privilege**: در این نوع از تهدیدها، کار سعی می‌کند با بدست آوردن دسترسی‌های سطح بالاتر در سیستم، یک فعالیت غیرمجاز در سیستم انجام دهد. به عنوان مثال به داده‌های غیرمجاز دست یابد یا به صورت غیرمجاز یکی از عملکردهای سیستم را فراخوانی کند. در این تهدید، مکانیزمهای دفاعی سیستم همانند مجازشماری و کنترل دسترسی، دور زده خواهد شد.

۲-۲-عاملین تهدید در سیستم سادا

با توجه به شناخت بدست آمده از سیستم، عوامل تهدید در سیستم سادا مشتمل بر ۷ گروه هستند که عناوین آنها در جدول ۱ آمده است.

جدول ۱: عاملین تهدید

شناسه عامل تهدید	عنوان عامل تهدید
TA01	کاربر بهره‌بردار سادا (SADA User)
TA02	کاربر مدیر سادا (SADA Admin)
TA03	کاربر مدیر ارشد سادا (SADA Super Admin یا همان Sys Admin)
TA04	مهاجمین داخلی
TA05	سرویس‌های دیگر
TA06	توسعه دهنده سادا (SADA Developer)، مدیر پایگاه‌داده، دیگر مدیران سیستم (به غیر از مدیر ارشد سادا)
TA07	پیمانکار Multi-AV

۳-۲-اهداف احتمالی مهاجمین در سیستم سادا

در جدول ۲ فهرست اهداف احتمالی مهاجمین در سیستم سادا، مشخص شده‌اند.

جدول ۲: اهداف مهاجمین

شناسه هدف	هدف
AG01	آپلود فایل‌های آلوده در هیولا
AG02	دسترسی غیرمجاز به داده‌های کاربران و پروژه‌ها
AG03	مخدوش کردن داده‌های کاربران و پروژه‌ها
AG04	استخراج غیرمجاز داده‌های ذخیره شده کاربران و پروژه‌ها به بیرون از شبکه سازمان
AG05	دور زدن کنترل‌های امنیتی
AG06	افزایش سطح دسترسی‌های کاربر بهره‌بردار به کاربر مدیر سادا و کاربر مدیر ارشد سادا
AG07	افزایش سطح دسترسی‌های کاربر مدیر سادا به کاربر مدیر ارشد سادا
AG08	از دسترس خارج کردن سرویس‌ها

۴-۲-آسیب‌پذیری‌های احتمالی سیستم سادا

در این بخش برخی از نقاط ضعف احتمالی موجود در سیستم سادا که می‌توانند مورد بهره‌برداری قرار گیرند و تهدیدهایی را متوجه سیستم کنند، آورده شده‌اند. این آسیب‌پذیری‌ها در جدول ۳ بیان شده‌اند.

جدول ۳: آسیب‌پذیری‌های احتمالی

شناسه آسیب‌پذیری	شرح آسیب‌پذیری
V01	به کارگیری credentialهای ضعیف برای کاربران
V02	عدم استفاده از مکانیزم MFA برای احرازهویت کاربران (مدیر سادا، مدیر ارشد سادا و کاربر بهره‌بردار)
V03	عدم الزام استفاده از پروتکل‌های TLS در برخی از ارتباطات همانند ارتباط با LDAP، ارتباط Rclone، ارتباط با FAM Driver، ارتباط با حافظ و غیره

V04	ذخیره‌سازی plaintext رمزهای عبور پایگاه داده‌ها و دیگر credentialها در فایل‌های پیکربندی
V05	عدم امنسازی پیکربندی سرویس‌ها و سیستم‌عامل‌ها
V06	عدم بررسی امکان دستکاری شدن imageها
V07	عدم بررسی محتوای فایلهای موجود در هیولای نامطمئن از نظر آلودگی
V08	امکان اتصال مستقیم USB Disk به سرور
V09	عدم وجود لاگ برای FAM
V10	عدم ممیزی دسترسی به فایلها و دایرکتوری‌های حساس همانند فایلهای پیکربندی و دایرکتوری ذخیره‌سازی کلیدها و certificateها
V11	عدم تنظیم درست مجوزهای دسترسی به فایلهای حساس همانند فایلهای پیکربندی
V12	عدم فعال بودن audit پایگاه‌داده‌ها
V13	عدم بررسی آدرسهای IP کاربران و همچنین زمان دسترسی آنها به سیستم
V14	عدم کافی بودن لاگهای موردنیاز از فعالیتهای کاربران در هیولا، حافظ و VMها
V15	عدم امکان revoke کردن توکنها توسط مدیر
V16	عدم وجود محدودیت روی تعداد توکن های فعال مورداستفاده توسط کاربران
V17	وجود آسیب‌پذیری در VM imageهای مورداستفاده
V18	وجود آسیب‌پذیری در مولفه‌های مختلف Open Stack
V19	وجود آسیب‌پذیری در مولفه‌های زیرساختی همانند سیستم‌عامل‌ها، دیتابیس‌ها و تکنولوژی‌های مجازی‌سازی همانند Docker
V20	عدم پایش و نظارت کافی روی تمام مولفه‌های سادا
V21	عدم وجود لاگ کافی از مولفه‌های مختلف سادا

V22	دسترسی کاربر مدیر سادا به فایلهای تمام کاربران دامنه تحت کنترل خود (مثلا از طریق حساب متمرکز قابل دسترس در حافظ)

۵-۲- فهرست تهدیدهای احتمالی

در این بخش، فهرست تهدیدهای احتمالی سیستم سادا که برمبنای اهداف مهاجمین، عاملین تهدید موجود در سیستم و آسیب‌پذیری‌های موجود آورده شده است. در تشریح هر تهدید، دسته‌بندی آن برمبنای چارچوب STRIDE، اثر آن تهدید و راهکارهای کاهش یا رفع آنها آورده شده است.

T01: تایید انتقال فایل‌های آلوده به محیط مطمئن در اثر خطای انسانی

با توجه به اینکه تایید یا رد درخواست انتقال فایل‌ها به محیط مطمئن توسط کاربر ادمین و به صورت دستی انجام می‌گیرد، بنابراین امکان وجود اشتباه انسانی در این فرایند وجود دارد. درواقع اگر به صورت سیستمی، از انتقال فایل‌هایی که توسط ماژول FAM، تگ فایل آلوده به آنها زده شده است، به محیط مطمئن جلوگیری نشود، امکان آلوده شدن محیط مطمئن وجود خواهد داشت.

اثر تهدید:

مهمترین اثر این تهدید، انتقال فایل‌های آلوده به هیولای محیط مطمئن است.

عاملین تهدید: TA02

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

بهتر است علاوه بر فراهم نمودن امکان تایید یا انتقال درخواستهای انتقال فایل به محیط مطمئن توسط کاربر مدیر سادا، به صورت سیستمی نیز از انتقال فایل‌هایی که تگ آلوده خورده‌اند، جلوگیری شود. البته بهتر است به طور کلی فایل‌های با تگ آلوده، در فهرست فایل‌های قابل تایید یا رد آورده نشوند.

T02: دستیابی و دستکاری فایل‌ها هنگام انتقال به هیولای مطمئن

در صورتی که ارتباط بین سرور انتقال فایل (حافظ) تا محیط مطمئن، برمبنای پروتکل TLS نباشد، ممکن است مهاجمین داخلی که توانسته‌اند به شبکه دست یابند، با شنود این ارتباط و دستکاری فایل‌ها، فایل‌های سالم را با فایل‌های آلوده جایگزین کنند. ضمنا حتی اگر این ارتباط TLS باشد، اما مثلا certificate آن منقضی شده باشد، باز هم امکان دسترسی کاربران شبکه به این فایل‌ها فراهم خواهد شد.

اثر تهدید:

مهمترین اثر این تهدید، انتقال فایل‌های آلوده به هیولای محیط مطمئن است.

عاملین تهدید: TA04

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

باید تمام ارتباطات موجود در سیستم به خصوص ارتباطات ماژول‌های امنیتی همانند FAM با سایر مولفه‌ها و همچنین ارتباطات منتهی به هیولای محیط مطمئن از نوع TLS باشند. ضمنا بهتر است، فایل‌ها قبل از انتقال به محیط مطمئن، رمزنگاری و امضا شوند تا در صورت دسترسی کاربران به کانال انتقالی، امکان خواندن و دستکاری آنها وجود نداشته باشد.

T03: دستکاری تگ فایل‌ها به صورت غیرمجاز در پایگاه داده FAM

در صورتی که اطلاعات مربوط به وضعیت پایش فایل‌ها همانند مقدار تگ فایل‌ها که در پایگاه‌داده درایور تحلیل بدافزار (FAM) ذخیره می‌شوند، توسط کاربران پایگاه داده همانند مدیر پایگاه‌داده، قابل رؤیت و ویرایش باشند، ممکن است این کاربران به عمد یا به اشتباه، این اطلاعات را دستکاری کنند.

اثر تهدید:

در صورتی که مدیر پایگاه داده تگ فایل را از وضعیت آلوده به وضعیت غیرآلوده تبدیل کند، امکان انتقال فایل‌های آلوده به هیولای محیط مطمئن وجود خواهد داشت.

عاملین تهدید: TA06

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

بهتر است اطلاعات مهمی همانند وضعیت پایش فایل‌ها که برمبنای آنها، تصمیم‌گیری‌هایی در سیستم انجام می‌شود، برای بقیه کاربران به غیر از سرویس FAM، به صورت read-only یا رمزشده در پایگاه داده ذخیره شوند و یا به کمک مکانیزمهای تشخیص صحت داده، از عدم دستکاری غیرمجاز آنها اطمینان حاصل کرد. ضمنا بهتر است audit log پایگاه داده FAM برای فراهم کردن امکان ردیابی فعالیتهای کاربران پایگاه‌داده فعال شده باشد.

T04: عدم تشخیص فایل‌های آلوده توسط ماژول FAM

در صورت عدم به‌روزرسانی signatureهای تشخیص بدافزار در ماژول FAM و یا پیکربندی نادرست این ماژول توسط پیمانکار مربوطه، احتمال عدم تشخیص فایل‌های آلوده قبل از انتقال به هیولای محیط مطمئن وجود خواهد داشت.

اثر تهدید:

مهمترین اثر این تهدید، انتقال فایل‌های آلوده به هیولای محیط مطمئن است.

عاملین تهدید: TA05 و TA07

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

signatureهای تشخیص بدافزار در ماژول FAM همواره باید به‌روز باشند. همچنین پیکربندی‌های موردنیاز در این ماژول باید توسط افراد مجاز و به درستی انجام شده باشد.

T05: استفاده از signatureهای دستکاری شده در ماژول Multi-AV

در صورتی که هیچ نوع بررسی در ماژول Multi-AV بر روی صحت signatureهای تشخیص بدافزار که از ریپازیتوری مرکزی آن دریافت می‌شود، انجام نشود، امکان دریافت signatureهای دستکاری شده وجود خواهد داشت.

اثر تهدید:

در این صورت، امکان عدم تشخیص فایل‌های آلوده توسط ماژول FAM وجود خواهد داشت.

عاملین تهدید: TA07

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

بهتر است هنگام دریافت signatureهای تشخیص بدافزار از ریپازیتوری مرکزی آن، امکان وارسی صحت آنها وجود داشته باشد.

T06: ذخیره‌سازی فایل‌های آلوده در هیولای نامطمئن

با توجه به اینکه هنگام تغذیه فایل‌ها در هیولای نامطمئن، هیچ نوع مکانیزمی جهت بررسی محتوای فایل‌های انتخابی از نظر آلودگی به بدافزار و مخرب بودن انجام نمی‌گیرد، احتمال ذخیره‌سازی فایل‌های آلوده در این محیط، بسیار بالاست.

اثر تهدید:

فایل‌های آلوده می‌توانند در انواع حملات مبتنی بر بدافزار، مورد بهره‌برداری قرار گیرند. حملات RCE[1]، نمونه‌ای از این حملات هستند. مهاجم می‌تواند این حملات را از طریق VMهای کاربران سادا، سرور حافظ و هر نقطه‌ای از سیستم سادا که فایلهای آلوده، قابل دسترس و اجرا شدن باشند، انجام دهد.

عاملین تهدید: TA02 و TA04

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

هرچند هدف اصلی سیستم سادا، اطمینان از عدم وجود داده‌های آلوده به بدافزار در هیولای محیط مطمئن است و امن بودن هیولای محیط نامطمئن، از اهداف این سیستم نیست، با این حال بهتر است جهت افزودن یک لایه امنیتی دیگر به سیستم، یک اسکن اولیه روی فایل‌ها قبل از انتقال به هیولای نامطمئن نیز صورت بگیرد تا از ذخیره‌سازی فایل‌های آلوده، در همان گام‌های ابتدایی آن پیشگیری شود.

T07: آلوده شدن سرور تغذیه فایل

با توجه به اینکه کاربر بهره‌بردار یا مدیر سادا، به طور مستقیم از USB Disk برای تغذیه فایل‌ها در هیولای نامطمئن استفاده می‌کنند، در صورتی که هیچ گونه بررسی روی فایل‌های موجود در این دیسک انجام نشود و مواردی همچون غیرفعال کردن قابلیت Autorun، انجام نشده باشد، آلوده شدن سرور تغذیه فایل با بدافزارهایی که حتی سخت‌افزار سرور را آلوده می‌کنند، قطعی است. علاوه بر این، در صورتی که این سرور به یک شبکه در سازمان وصل باشد، امکان گسترش این آلودگی در آن شبکه نیز وجود خواهد داشت. ضمنا در صورتی که اطلاعات و فایلهای حساسی در USB Disk ذخیره شده باشد، با مفقود شدن این دیسک، در صورتی که این اطلاعات رمزنگاری نشده باشند، ممکن است مورد سوءاستفاده قرار گیرند.

اثر تهدید:

با آلوده شدن سرور تغذیه، امکان از کار افتادن این سرور و حتی آلوده شدن سرورهای دیگری که با آن در ارتباط باشند، وجود دارد.

[1] Remote Code Execution

عاملین تهدید: TA02 و TA04

دسته‌بندی STRIDE: Tampering، Information-Disclosure

راهکار رفع یا کاهش اثر تهدید:

بهتر است قبل از انتقال فایلها از USB disk به سرور تغذیه، یک اسکن اولیه روی آن انجام شود. همچنین قابلیت Autorun در سیستم‌عامل غیرفعال گردد و پالیسی‌های مناسب جهت استفاده از این دیسک‌ها تعیین و اعمال شود. علاوه بر این، در صورتی که فایلهای حساسی در دیسک ذخیره شده باشد، بهتر است رمزنگاری شوند. در نهایت، قابلیت‌هایی همچون احرازهویت از طریق اثرانگشت برای دسترسی به سرور فعال شود.

T08: سرقت credentialها یا بدست آوردن توکن‌های معتبر دسترسی کاربران و سرویس‌ها

در صورت عدم بکارگیری پروتکل مبتنی بر TLS در ارتباط بین Keystone و سرور LDAP، امکان شنود این ارتباط توسط مهاجمین داخلی که به شبکه دست یافته‌اند، و در نتیجه دستیابی به credentialهای کاربران بهره‌بردار، مدیر سادا و مدیر ارشد سادا وجود خواهد داشت.

از طرف دیگر، در صورتی که ارتباط بین Keystone و مولفه‌هایی همانند وب‌اپلیکیشن حافظ، VM کاربر بهره‌بردار، Horizon و Swift Proxy برمبنای پروتکل TLS نباشد، امکان شنود این ارتباطات و دستیابی به credentialها و توکن‌های دسترسی صادر شده توسط Keystone وجود خواهد داشت.

در صورت عدم بکارگیری پروتکل TLS در ارتباط بین درایور تحلیل بدافزار (FAM) و Swift Proxy، ارتباط بین سرور حافظ و FAM، ارتباط بین FAM و Multi-AV و همچنین ارتباط بین حافظ و هیولای محیط مطمئن، احتمال شنود این ارتباط توسط مهاجمین داخلی و دستیابی به credentialهای ردوبدل شده فراهم خواهد شد.

همچنین در صورتی که توکن‌های دسترسی کاربران، سمت کلاینت مثلا در مرورگر ذخیره شده باشند، با دسترسی مهاجم به کلاینت، این اطلاعات نیز قابل دسترس خواهد بود. ذخیره‌سازی credentialهای کاربر بهره‌بردار به صورت متن‌واضح در کلاینت‌های RDP ، VNC و SPICE نیز همین تهدید را به دنبال خواهد داشت.

ضمنا در صورتی ه مهاجم بتواند به پایگاه داده Keystone و نیز فایل keystone-start.sh دست یابد، می‌تواند به credentialهای کاربر مدیر ارشد سادا است، دست یابد.

ذخیره‌سازی credentialهای کاربر بهره‌بردار در فایل پیکربندی Rclone به صورت plaintext و دستیابی مهاجمین به این فایل نیز این تهدید را به دنبال خواهد داشت.

همچنین در صورتی که credentialهای دسترسی به پایگاه داده‌ها به صورت plaintext در فایل‌های پیکربندی سرویس‌ها همانند فایل mysql-ready.sh ذخیره شوند، دسترسی مهاجم به این فایل‌ها، منجر به دسترسی به پایگاه داده‌ها خواهد شد.

ذخیره‌سازی پسوردهای مربوط به service accountهای سرویس‌های Openstack به صورت plaintext در فایل‌های پیکربندی مربوطه، نیز این تهدید را به دنبال خواهد داشت.

اثر تهدید:

این تهدید، با توجه به نوع دسترسی‌های کاربر یا سرویسی که مهاجم توانسته است به اطلاعات credentialها یا توکن‌های دسترسی آنها دست یابد، اثرات مختلفی بر روی سیستم خواهد داشت. به عنوان مثال در صورتی که credentialهای کاربر مدیر ارشد سادا در دست مهاجم باشد، احتمال دستکاری غیرمجاز پیکربندی کل زیرساخت سادا و از دسترس خارج شدن آن، فراهم خواهد بود. کافی است این کاربر، سرویس Keystone را ریستارت کند؛ در حین ریستارت این سرویس، مکانیزم احرازهویت و مجازشماری در دسترس نخواهد بود. یا مثلا در صورتی که مهاجم بتواند به credentialهای دسترسی به APIهای سرویس‌های OpenStack دست یابد، می‌تواند این APIها را فراخوانی کرده و مثلا سرویس‌ها را دستکاری کند.

عاملین تهدید: TA04، TA01، TA02، TA03

دسته‌بندی STRIDE: Spoofing

راهکار رفع یا کاهش اثر تهدید:

اولا بهتر است تمام ارتباطات موجود در سیستم از جمله ارتباط بین Keystone و سرور LDAP، از نوع TLS باشند که در ادامه لینک‌های راهنمای مربوطه آورده شده است:

- لینک راهنمای امنسازی بین Keystone و سرور LDAP
- لینک راهنمای امنسازی ارتباط با پایگاه داده‌ها
- لینک راهنمای امنسازی ارتباطات سرویس Neutron
- لینک راهنمای امنسازی ارتباطات سرویس Glance
- لینک راهنمای امنسازی ارتباطات سرویس Nova
- لینک راهنمای تنظیم سرآیند امنیتی HSTS در پاسخ‌های بازگشتی از Horizon
- لینک راهنمای امنسازی ارتباطات RabbitMQ

ثانیا، حداقل برای مدیران سادا و مدیران ارشد سادا، بهتر است از مکانیزم MFA[1] برای ورود به سیستم استفاده شود (لینک راهنما). همچنین در صورت امکان، بهتر است آدرس IP کاربران و حتی روزها و ساعت‌هایی که می‌توانند از سیستم استفاده کنند نیز به عنوان پارامترهایی در فرایند احرازهویت در نظر گرفته شوند. این راهکار امکان تشخیص فعالیت‌های مخرب کاربران را فراهم می‌کند.

در صورت امکان بهتر است قابلیت TLS client authentication برای دسترسی سرویس‌ها به یکدیگر هم فعال شود تا یک لایه امنیتی دیگر علاوه بر نام کاربری و پسورد اختصاص داده شده به service accountها اضافه شود. البته در این حالت، سربار و هزینه صدور گواهی TLS برای سرویس وجود خواهد داشت.

علاوه بر این، بهتر است امکان مشاهده نشست‌های کاربران و revoke کردن توکن‌های مربوطه برای کاربر مدیر سادا وجود داشته باشد. برای revoke کردن توکن‌های Fernet کافی است که key repository موجود، حذف و مجموعه کلیدهای جدیدی ایجاد و در همه نودهای کلاستر توزیع شوند. علاوه بر این، امکان revoke کردن توکن‌ها از طریق API سرویس Keystone نیز وجود دارد.

ضمنا بهتر است توکن ادمین که برای آغاز به کار سرویس Keystone به کار می‌رود، غیرفعال شود (لینک راهنما). همچنین سرویس Swift نیز با مجوز دسترسی non-root اجرا شود (لینک راهنما)

قابلیت Autocomplete برای فیلد پسورد در داشبورد Horizon منجر به ذخیره‌سازی پسورد کاربران در مرورگر می‌شود، به همین دلیل بهتر است غیر فعال شود (لینک راهنما). علاوه بر این، در صورتی که از کوکی‌ها برای ذخیره‌سازی توکن‌های کاربران سمت مرورگر استفاده شود، هم در Horizon و هم وب‌اپلیکیشن حافظ، بهتر است نکات امنسازی کوکی‌ها همانند تنظیم فلگ HTTP-Only و Secure برای آنها انجام شده باشد (لینک راهنما برای داشبورد Horizon).

T09: حدس زدن credentialهای کاربران

در صورتی که سمت سرور LDAP از پالیسی‌های ضعیفی برای ایجاد credentialهای کاربران استفاده شده باشد، امکان حدس زدن آن برای مهاجمین داخلی و دیگر کاربران فراهم خواهد بود. به عنوان مثال، در برخی از سازمان‌ها، برای نام کاربری افراد، از یک ساختار مشخص همانند نام واحد سازمانی به عنوان پیشوند و کد پرسنلی به عنوان پسوند، استفاده می‌شود که حدس زدن آن کار سختی نیست. بنابراین مهاجم با استفاده از تکنیک‌هایی همانند Brute Force، امکان تست ورود به سیستم را با نام‌های کاربری معتبر خواهد داشت. در صورتی که کلمه عبور بکار رفته نیز ساده باشد، امکان دسترسی به حساب کاربری قبل از قفل شدن آن توسط مکانیزم قفل حساب کاربری، فراهم خواهد بود.

اثر تهدید:

[1] Multi-Factor Authentication

اثر این تهدید همانند تهدید T08 است.

عاملین تهدید: TA04، TA01، TA02، TA03

دسته‌بندی STRIDE: Spoofing

راهکار رفع یا کاهش اثر تهدید:

در صورت امکان، بهتر است از مکانیزم کپچا علاوه بر مکانیزم قفل حساب کاربری، برای محدود کردن امکان اجرای تکنیک‌های Brute Force برای بدست آوردن نامهای کاربری و کلمات عبور معتبر کاربران، استفاده شود. ضمنا بهتر است حداقل برای مدیران سادا و مدیران ارشد سادا، از مکانیزم MFA نیز استفاده شود. همچنین در صورت امکان، بهتر است آدرس IP کاربران و سرویس‌ها و حتی روزها و ساعت‌هایی که کاربر می‌تواند از سیستم استفاده کند، نیز به عنوان پارامترهایی در فرایند احرازهویت در نظر گرفته شوند.

T10: جعل هویت کاربران با دسترسی به کلیدهای Fernet

در صورتی که مهاجم بتواند به key repository شامل کلیدهای مورداستفاده برای رمزنگاری توکن‌های Fernet دست یابد، به کمک این کلیدها می‌تواند توکن‌های معتبری تولید کند و از آنها برای دسترسی به سیستم استفاده نماید. تا زمانی که این کلیدها از key repository حذف نشوند، امکان استفاده از آنها برای تولید توکن‌های جدید همچنان وجود خواهد داشت.

اثر تهدید:

در صورتی که مهاجم شناسه ادمین یک پروژه را بداند و به کلیدهای Fernet نیز دسترسی داشته باشد، امکان تولید توکن‌های دسترسی ادمین برای او فراهم خواهد بود. به کمک این توکن، مهاجم می‌تواند به تمام پروژه‌های تحت مدیریت ادمین دست یابد.

عاملین تهدید: TA04، TA03

دسته‌بندی STRIDE: Spoofing

راهکار رفع یا کاهش اثر تهدید:

بهتر است فرایند Key rotation برای تنزل کلیدهای primary مورداستفاده برای رمزنگاری توکن‌های Fernet به کلیدهای secondary و تولید کلیدهای جدید انجام شود. در این صورت اگر کلید primary قبلی به دست مهاجم افتاده باشد، امکان استفاده از آن برای تولید توکن جدید وجود نخواهد داشت. هرچند که امکان رمزگشایی توکن‌های قبلی همچنان وجود خواهد داشت. ضمنا مجوزهای دسترسی به key repository نیز باید به درستی تنظیم شود. این دایرکتوری فقط باید توسط سرویس Keystone قابل دسترس (خواندن و نوشتن) باشد.

T11: افشای secretهای مورداستفاده سرویس‌ها

با توجه به اینکه secretهای مورداستفاده سرویس‌ها به صورت plain text در فایل‌های پیکربندی آنها، ذخیره و هاردکد شده‌اند، با دستیابی به این فایل‌ها امکان دسترسی به این secretها نیز فراهم خواهد شد. این secretها شامل کلمات عبور دسترسی به سرویس‌های دیگر، کلمات عبور دسترسی به پایگاه داده‌ها، کلیدهای رمزنگاری objectها، API keyها و certificateها هستند.

اثر تهدید:

با دستیابی به این secretها امکان سوءاستفاده از آنها برای دستیابی به داده‌های غیرمجاز یا دور زدن مکانیزم‌های امنیتی فراهم خواهد شد. با توجه به نوع secret مورد دسترس، مهاجم می‌تواند فعالیت‌های مخرب مختلفی انجام دهد. به عنوان مثال، در صورت دسترسی مهاجم به کلمه عبور پایگاه‌داده‌ها، امکان دسترسی غیرمجاز به داده‌های موجود در این پایگاه داده‌ها فراهم خواهد شد. در برخی از موارد حتی امکان دسترسی به سایر سرویس‌های سازمانی همانند LDAP نیز فراهم می‌شود. به عنوان مثال، در صورتی که مهاجم بتواند به فایل پیکربندی Keystone دست یابد، می‌تواند از کلمه عبوری که برای دسترسی این سرویس به LDAP در نظر گرفته شده است، آگاه شود. حال اگر، این کاربر در سرور LDAP، مجوز دسترسی تغییر هم داشته باشد، علاوه بر سرویسهای OpenStack مهاجم می‌تواند سرور LDAP را نیز مورد حمله قرار دهد (در این لینک و این لینک می‌توان این موضوع را مطالعه کرد).

عاملین تهدید: TA04، TA03

دسته‌بندی STRIDE: Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

بهتر است secretها به صورت رمزشده در فایل‌های پیکربندی ذخیره شوند. اما بهترین راهکار آن است که از یک سیستم مدیریت متمرکز secretها برای نگهداری این داده‌ها استفاده شود. سرویس Barbican یکی از سرویس‌های OpenStack است که امکان مدیریت متمرکز secretها را برای سایر سرویس‌های OpenStack فراهم می‌کند. برای دستیابی یا ذخیره‌سازی یک secret در این سیستم، لازم است ابتدا کاربر در سیستم Keystone احرازهویت شود.

استفاده از سیستم Barbican مزایایی همانند کنترل دسترسی به secretها برمبنای پالیسی‌های تعریف شده، اعمال quota، امکان تنظیم لیست ACL به ازای هر secret، گروه‌بندی secretها و ردیابی استفاده‌کنندگان از secretها را فراهم می‌کند. البته ناگفته نماند که این سرویس می‌تواند با سیستم‌های خارجی همانند Hashicorp Vault، KMIP و دیگر سیستم‌هایی که پلاگین آنها در OpenStack موجود است، نیز ادغام شود. برای این منظور کافی است که در backend، APIهای ارائه شده این سیستم‌ها را فراخوانی کند. البته امکان

ذخیره‌سازی secretها در پایگاه‌داده خود سرویس Barbican نیز وجود دارد، اما استفاده از سیستم‌های خارجی امکان ذخیره‌سازی secretها را در یک سیستم کاملا منفک فراهم می‌کند.

T12: دستکاری غیرمجاز فایل‌های پیکربندی و دایرکتوری‌های حساس

در صورتی که مجوزهای دسترسی به فایل‌های پیکربندی سرویس‌ها و دایرکتوری‌های حساسی همانند key repository حاوی کلیدهای رمزنگاری توکن‌های Fernet و همچنین دایرکتوری‌های حاوی TLS Certificateها به درستی تنظیم نشده باشد، امکان دستکاری آنها توسط کاربران غیرمجاز فراهم خواهد شد.

اثر تهدید:

دستکاری غیرمجاز فایل‌های پیکربندی سرویس‌های Openstack امکان تهدیدهای بسیاری از جمله از دسترس خارج شدن این سرویس‌ها، غیرفعال کردن مکانیزم احرازهویت، پیکربندی نادرست مکانیزم کنترل دسترسی، غیرفعال کردن مکانیزم رمزنگاری اشیاء و دیگر تهدیدات را به دنبال خواهد داشت. در مورد فایل‌های پیکربندی سایر سرویس‌ها و پروتکل‌ها همانند Rclone، FAM و پایگاه‌داده‌ها نیز، دستکاری غیرمجاز آن منجر به تهدیدهای مرتبط خواهد شد. به عنوان مثال دستکاری غیرمجاز فایل Rclone می‌تواند منجر به تغییر دسترسی کاربر از read-only به دسترسی نوشتن در هیولا شود که در محیط مطمئن، غیرمجاز است.

عاملین تهدید: TA03، TA04 و TA06

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

به طور کلی در اعطای دسترسی‌ها باید اصل حداقل دسترسی در نظر گرفته شده باشد و باید مجوزهای دسترسی فایل‌های پیکربندی به درستی تنظیم شود. در لینک‌های زیر نحوه تنظیم درست این مجوزها برای سرویس‌های OpenStack آورده شده است:

- لینک راهنمای تنظیم مالکیت و مجوزهای دسترسی فایل‌های پیکربندی Keystone
- لینک راهنمای تنظیم مالکیت و مجوزهای دسترسی فایل‌های پیکربندی Neutron
- لینک راهنمای تنظیم مالکیت و مجوزهای دسترسی فایل‌های پیکربندی Nova
- لینک راهنمای تنظیم مالکیت و مجوزهای دسترسی فایل‌های پیکربندی Swift
- لینک راهنمای تنظیم مالکیت و مجوزهای دسترسی فایل‌های پیکربندی Glance
- لینک راهنمای تنظیم مالکیت و مجوزهای دسترسی فایل‌های پیکربندی Horizon

در صورت امکان هم بهتر است با استفاده از یک راهکار FIM[1]، دسترسی به این فایلها و تغییرات آنها به طور منظم پایش شود (لینک راهنما). همچنین بهتر است چارچوب‌های کنترل دسترسی MAC[2] همانند SELinux در سیستم‌عامل سرور فعال و پیکربندی شود.

T13: دسترسی غیرمجاز به هیولا و سایر سرویس‌ها

با توجه به اینکه امکان استفاده از سرویس‌های OpenStack بدون انجام احرازهویت و برمبنای استراتژی noauth وجود دارد، در صورت عدم بررسی پیکربندی سرویس‌ها، امکان تنظیم این استراتژی در آنها وجود خواهد داشت.. از طرف دیگر، در صورتی که استراتژی Keystone برای احرازهویت استفاده باشد، اما پیکربندی، گروه‌ها، نقش‌ها و دسترسی‌ها، به درستی انجام نشده باشد، امکان دسترسی نادرست و غیرمجاز به سرویس‌ها فراهم خواهد شد.

در صورت پیکربندی نادرست ACLها برای کیسه‌ها، امکان دسترسی غیرمجاز به objectها نیز فراهم خواهد بود. ضمنا در صورت دستیابی غیرمجاز کاربر به دیسک، امکان دستیابی به objectها فراهم خواهد شد. اما چون داده‌ها در هیولا به صورت رمزشده نگهداری می‌شوند، امکان افشای آنها میسر نیست، هرچند امکان دستکاری آنها فراهم خواهد بود.

در مورد سیستم احرازهویت و کنترل دسترسی مولفه FAM نیز در صورت عدم پیکربندی درست آن، امکان دسترسی غیرمجاز به API این مولفه فراهم خواهد شد.

اثر تهدید:

اثرات این تهدید، همانند تهدید T08 است.

عاملین تهدید: TA03، TA02، TA04 و TA06

دسته‌بندی STRIDE: Spoofing، Tampering و Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

بهتر است پیکربندی سرویس‌ها برای اطمینان از تنظیم درست استراتژی احرازهویت، مورد ممیزی قرار گیرد و این اطمینان حاصل شود که تمام سرویس‌های سادا، از مکانیزم Keystone برای احرازهویت استفاده می‌کنند. در لینک‌های زیر، پیکربندی سرویس‌های OpenStack آورده شده است:

- لینک راهنمای پیکربندی استراتژی مکانیزم احرازهویت Neutron

[1] File Integrity Monitoring

[2] Mandatory Access Control

- لینک راهنمای پیکربندی مکانیزم احرازهویت Swift
- لینک راهنمای پیکربندی مکانیزم احرازهویت Glance
- لینک راهنمای پیکربندی مکانیزم احرازهویت Nova

ضمنا در اعطای دسترسی‌های نقش‌ها به گروه‌ها و کاربران بهتر است، اصل حداقل دسترسی[1] در نظر گرفته شود و از اعطای دسترسی‌های بیش از حد نیاز خودداری شود.

T16: بهره‌برداری از آسیب‌پذیری‌های احتمالی موجود در مولفه‌ها و تکنولوژی‌های مورداستفاده

در صورتی که مولفه‌ها و تکنولوژی‌های مورداستفاده برای توسعه و استقرار سیستم سادا، حاوی آسیب‌پذیری باشند، امکان بهره‌برداری از این آسیب‌پذیری‌ها برای مهاجمین فراهم خواهد داشت.

اثر تهدید:

اثر وجود آسیب‌پذیری‌ها در تکنولوژی‌های مورداستفاده، با توجه به آن تکنولوژی و محل استفاده آن و همچنین نوع آسیب‌پذیری می‌تواند متفاوت باشد. در این لینک، فهرستی از آسیب‌پذیری‌های مختلفی که در سالهای اخیر بر روی سرویس‌های مختلف Openstack گزارش شده است به همراه اثر آنها آورده شده است.

عاملین تهدید: TA06، TA05، TA04 و TA07

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

بهتر است فهرست کاملی از تکنولوژی‌های مورداستفاده برای توسعه و استقرار سادا به همراه اطلاعاتی شامل محل استفاده تکنولوژی، نسخه مورداستفاده، لایستس مربوطه، آخرین وضعیت پشتیبانی و در نهایت فهرست آسیب‌پذیری‌هایی که تاکنون شناسایی شده‌اند، تهیه شود[2]. سپس وصله‌های موردنیاز برای آسیب‌پذیری‌ها نصب شوند.

در حال حاضر ابزارهایی وجود دارند که امکان اسکن خودکار آسیب‌پذیری‌های تکنولوژی‌ها را فراهم کرده‌اند. به عنوان مثال برای اسکن خودکار آسیب‌پذیری‌های docker containerها می‌توان از ابزارهای Container scanning همانند Trivey و Anchore استفاده کرد.

در مورد FAM که توسط شرکت‌های شخص ثالث توسعه داده می‌شود نیز بهتر است فهرست مولفه‌ها و تکنولوژی‌های مورداستفاده به همراه اطلاعات موردنیاز ارائه شود.

---

[1] Least privilege

[2] در توسعه امن نرم‌افزار، به این فهرست، Software Bill Of Materials یا به اختصار SBOM گفته می‌شود.

T17: از دسترس خارج شدن سرویس‌ها

در صورتی که پیکربندی‌های سرویس‌های سادا به درستی انجام نشده باشد و یا بعدا به عمد یا غیرعمد توسط کاربر ارشد سادا یا مهاجمین داخلی، دستکاری شوند، می‌توانند منجر به از دسترس خارج شدن آن سرویس شوند. به عنوان مثال، در صورتی که حداکثر اندازه body درخواست‌های ارسالی به Keystone مشخص و محدود نشده باشد، مهاجم می‌تواند با ارسال درخواست‌هایی با اندازه بزرگ، منجر به از کار افتادن این سرویس شود. یا در مثالی دیگر، فعال نمودن قابلیت LDAP debugging در پیکربندی Keystone در محیط production منجر به ایجاد تاثیر منفی بر روی کارایی سیستم خواهد داشت.

با توجه به اینکه در حال حاضر، فرایند هاردنینگ و اعمال best practiceهای امنیتی برای همه سرویس‌ها انجام نشده است، همچنین دسترسی به فایل‌های پیکربندی و ایجاد تغییرات در آنها نیز مورد پایش قرار نمی‌گیرد، بنابراین امکان دستکاری این فایل‌ها وجود دارد که در نتیجه آن با توجه به نوع سرویس، عملکرد مربوطه نیز می‌تواند مختل شود.

حذف عمدی یا غیرعمدی کلیدهای secondary توکن‌های Fernet که برای رمزگشایی توکن‌های موجود استفاده می‌شوند نیز می‌تواند منجر به ایجاد شکست در احرازهویت کاربران با توکن‌های موجود و معتبر شود.

ایجاد مشکل در لینک ارتباطی بین مولفه‌ها نیز از جمله مواردی است که می‌تواند منجر به از دسترس خارج شدن سرویس‌ها شود.

اثر تهدید:

با توجه به نوع سرویسی که ممکن است از دسترس خارج شود، تبعات مختلفی می‌تواند برای سادا وجود داشته باشد. به عنوان مثال در صورتی که سرویس Keystone از دسترس خارج شود، سیستم احرازهویت و کنترل دسترسی سادا، مختل خواهد شد.

عاملین تهدید: TA03، TA04 و TA06

دسته‌بندی STRIDE: Tampering، Denial of Service

راهکار رفع یا کاهش اثر تهدید:

اولا بهتر است مجوزهای دسترسی به فایل‌های پیکربندی سرویس‌ها و key repository توکن‌های Fernet و امکان ایجاد هر نوع تغییر در آنها، طبق best practiceهای مربوطه تنظیم و کنترل شوند. ثانیا موضوع health check سرویس‌ها نیز به مداوم و منظم انجام شود و برمبنای آن، در صورت مشاهده هر نوع اختلال در عملکرد سرویس، بلافاصله به کاربران ادمین مربوطه اطلاع‌رسانی شود.

بهتر است حداکثر اندازه body درخواست‌های ارسالی به Keystone مشخص و محدود شده باشد (لینک راهنما).

علاوه بر این، بهتر است در تعیین حداکثر تعداد کلیدهای فعال موردنیاز برای رمزگشایی توکن‌های Fernet، پارامتر token_expiration و rotation_frequency در نظر گرفته شود تا حداقل از حذف غیرعمد کلیدها، جلوگیری شود. در این لینک نحوه محاسبه آن آورده شده است.

T18: استفاده از imageهای دستکاری شده برای ایجاد VMها

در صورتی که ارتباط بین سرویس‌های Glance و Nova برمبنای TLS نباشد، امکان دستکاری imageها هنگام انتقال بین Glance و Nova وجود خواهد داشت. علاوه بر این، در صورتی که مجوزهای دسترسی دایرکتوری imageها به درستی تنظیم نشده باشد، امکان دستکاری آنها وجود خواهد داشت. البته ناگفته نماند که هنگام بوت شدن image جدید، یک بررسی با checksum اولیه آن انجام می‌شود، اما در صورتی که دفعات بعدی از همان image استفاده شود، این بررسی انجام نمی‌شود. بنابراین در صورت دستکاری imageها، کاربر از آن مطلع نخواهد شد.

اثر تهدید:

با دستکاری imageها، امکان قرار دادن بدافزارها و rootkitها در آنها وجود خواهد داشت.

عاملین تهدید: TA02، TA03، TA04 و TA06

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

برای کاهش این تهدید می‌توان از قابلیت image signature verification که توسط سرویس Glance ارائه می‌شود، استفاده کرد. درواقع کاربر می‌تواند image موردنظرش را با استفاده از کلید خصوصی‌اش امضا کند. سپس image و امضای دیجیتال آن را به همراه اطلاعات مربوط به محل ارجاع کلید عمومی مربوطه، آپلود کند. پس از آن سرویس Glance می‌تواند امضای imageها را برمبنای این اطلاعات بررسی کند و نتیجه را به کاربر اطلاع دهد. البته این روش برای حالتی است که کاربر خود برای image موردنظرش یک امضا تولید می‌کند. در حالت‌های دیگر امکان تولید امضا برای imageها توسط سرویس‌های Nova و Glance نیز وجود دارد.

T19: دسترسی غیرمجاز به پایگاه داده‌های مولفه‌های مختلف سادا

با توجه به اینکه credentialهای دسترسی به پایگاه داده‌ها به طور plaintext در فایل‌های پیکربندی ذخیره می‌شوند، در صورت دسترسی مهاجم به این فایل‌ها امکان استفاده از این اطلاعات برای ورود به سیستم پایگاه‌داده و دستیابی به داده‌های سرویس‌ها فراهم خواهد شد. شرایط وقتی بدتر می‌شود که حساب کاربری

این سرویس در پایگاه داده، دسترسی کامل برای ایجاد و حذف پایگاه داده داشته باشد. از طرف دیگر، با توجه به اینکه audit log سیستم‌های پایگاه داده نیز فعال نشده است، امکان شناسایی کامل فعالیت‌های کاربران پایگاه‌داده وجود نخواهد داشت.

اثر تهدید:

با توجه به سرویس موردنظر، دسترسی غیرمجاز به پایگاه داده آن می‌تواند تبعات مختلفی از جمله دستکاری اطلاعات مرتبط با فهرست مشخصات کاربران (به خصوص کاربران ارشد سادا)، مشخصات objectها همانند آدرس محل قرارگیری آنها در containerها، تعداد objectهای موجود در containerها، نتایج اسکن فایل‌ها توسط FAM، اطلاعات مرتبط با imageها شامل مشخصات آنها، ویژگی‌های آنها و محل قرارگیری آنها و غیره به دنبال داشته باشد. در صورتی که کاربر دسترسی full داشته باشد، حتی می‌تواند پایگاه‌داده را حذف کند که این خود می‌تواند منجر به از دسترس خارج شدن سرویس مربوطه خواهد شد.

عاملین تهدید: TA03 و TA04 و TA06

دسته‌بندی STRIDE: Spoofing ،Tampering

راهکار رفع یا کاهش اثر تهدید:

بهتر است اطلاعات دسترسی به پایگاه داده‌ها به صورت رمزشده در فایل‌های پیکربندی ذخیره شوند. البته در صورت استفاده از سیستم متمرکز کلیدها و پسوردها، بهتر است این credentialها در این سیستم، ذخیره و بازیابی شوند.

در صورت امکان بهتر است راهکار TLS Client Authentication برای ایجاد یک فاکتور دوم در فرایند احرازهویت، علاوه بر نام کاربری و کلمه عبور نیز استفاده شود (لینک راهنما). ضمنا مجوزهای دسترسی اعطا شده به حساب کاربری اختصاص داده شده به سرویس‌ها در سیستم پایگاه داده‌ها حاوی حداقل دسترسی‌های موردنیاز باشد و از اعطای دسترسی full به این حساب‌ها پرهیز شود.

همچنین بهتر است audit log سیستم‌های مدیریت پایگاه داده‌ها برای ثبت دسترسی‌های کاربران فعال شده باشد.

T20: دسترسی غیرمجاز به VMها از طریق SPICE/VNC و RDP

با توجه به اینکه در سیستم سادا، برای دسترسی از راه دور به VMها، از مکانیزم احرازهویت LDAP در ارتباطات مبتنی بر SPICE/VNC استفاده می‌شود، در صورتی که مهاجم بتواند به اطلاعات credential کاربر در LDAP دست یابد، امکان دسترسی به VM او نیز فراهم خواهد شد. در مورد ارتباط از راه دور با VM، برمبنای RDP نیز در صورتی که از کلمات عبور قوی استفاده نشود، امکان بدست آوردن آنها برای مهاجم فراهم خواهد بود.

در صورتی که برای دسترسی به کنسول VM از پروتکل‌های رمزنشده استفاده شود، امکان شنود اطلاعات ردوبدل شده در ارتباط بین کلاینت و سرور، برای مهاجمین داخلی فراهم خواهد شد.

اثر تهدید:

در اثر این تهدید، امکان دسترسی مهاجمین و کاربران غیرمجاز به VMهای دیگر کاربران وجود خواهد داشت که در نتیجه آن امکان مشاهده داده‌های آنها در هیولا برایشان فراهم خواهد شد.

عاملین تهدید: TA03، TA04 و TA06

دسته‌بندی STRIDE: Spoofing و Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

پیکربندی مکانیزم احرازهویت MFA در Keystone و اطمینان از بکارگیری کلمات عبور قوی برای کاربران و پیاده‌سازی خط‌مشی‌های قفل حساب کاربری پس از عبور از حدآستانه تلاش‌های ناموفق، از راهکارهایی هستند که برای کاهش این تهدید باید در نظر گرفته شوند.

طبق مستندات OpenStack برای استفاده از هریک از تکنولوژی‌های VNC، SPICE یا RDP، لازم است سرویس پراکسی مربوطه، پیکربندی شود. در پیکربندی سرویس پراکسی، برای انتقال داده‌ها بین کلاینت و پراکسی بهتر است از پروتکل TLS استفاده شود. همچنین ارتباط بین سرور پراکسی و instance (VM) نیز باید به صورت رمزشده باشد که برای این منظور لازم است سمت VM و سرور پراکسی، نیز پیکربندی‌های موردنیاز انجام شود.

علاوه بر این، بهتر است پورت‌های مجاز instance برای استفاده در دسترسی از راه دور، با توجه به تکنولوژی مورداستفاده برای دسترسی از راه دور، در قالب قوانینی به فایروال instance و حتی security group پروژه اضافه شده باشند. آدرس‌های IP مجاز برای دسترسی از راه دور نیز بهتر است در فایروال و security group آن مشخص شوند.

T21: عدم تشخیص فعالیت‌های مخرب کاربران به دلیل وجود لاگ ناکافی

در صورتی که لاگ کافی از رویدادهای امنیتی و فعالیت‌های کاربران سادا در بخش‌های مختلف آن وجود نداشته باشد، امکان پایش و ممیزی این فعالیت‌ها و تشخیص رفتارهای غیرعادی وجود نخواهد داشت. علاوه بر این، در صورت وقوع یک حادثه امنیتی، بدون وجود لاگ کافی، تحلیل علت حادثه دشوار خواهد بود. طبق بررسی‌های انجام شده، در حال حاضر لاگ کافی در برخی از مولفه‌ها و سرویس‌های سادا تولید نمی‌شود. به عنوان مثال در مورد دسترسی به فایل‌ها و دایرکتوری‌های حساس، هیچ لاگی تولید نمی‌شود.

اثر تهدید:

مهمترین اثر این تهدید، عدم تامین ویژگی عدم انکار[1] است که یکی از ویژگی‌های امنیتی است که در آن کاربر امکان انکار کردن فعالیت انجام شده را ندارد. عدم تشخیص فعالیت‌های مخرب و همچنین عدم امکان تحلیل ریشه‌ای حوادث امنیتی، از اثرات نبود لاگ کافی از رویدادهای امنیتی و فعالیت‌های کاربران است.

عاملین تهدید: TA06 و TA07

دسته‌بندی STRIDE: Repudiation

راهکار رفع یا کاهش اثر تهدید:

به طور کلی برای کاهش این تهدید پیشنهاد می‌شود یک خط مشی مشخص، دقیق، کامل و توافق‌شده برای تعیین موارد زیر تعریف و پیاده‌سازی شود:

- تعیین منابعی که لاگ آنها باید جمع‌آوری شود.
- تعیین رویدادهای امنیتی که باید لاگ شوند و همچنین فیلدهای اطلاعاتی هر رویداد
- تعیین و اجرای قوانین کنترل دسترسی به لاگها
- پایش دسترسی‌ها
- انتقال تمام لاگ‌ها به سرور ELK
- در صورت امکان، کاهش تعداد log readerها برای کاهش سطح حمله

T22: دسترسی غیرمجاز به لاگ‌ها

در صورتی که قوانین دسترسی به لاگ‌ها به درستی پیکربندی و کنترل نشود، امکان دسترسی غیرمجاز به این داده‌ها برای افراد غیرمجاز فراهم خواهد شد.

اثر تهدید:

دسترسی غیرمجاز به داده‌های لاگ، امکان دستیابی به اطلاعات مهمی که از طریق این داده‌ها قابل استنتاج هستند، همانند اطلاعات ورود و خروج کاربران، را فراهم می‌کند. همچنین در صورتی که مجوزهای خواندن و نوشتن آنها به درستی تنظیم نشده باشد، امکان دستکاری این داده‌ها نیز فراهم خواهد شد که در نتیجه آن اثراتی که برای تهدید T21 برشمرده شد، در اینجا نیز مصداق خواهند داشت.

عاملین تهدید: TA03، TA04

دسته‌بندی STRIDE: Tampering، Information Disclosure و Repudiation

[1] Non-Repudiation

راهکار رفع یا کاهش اثر تهدید:

راهکار ارائه شده برای تهدید T21 در اینجا نیز مصداق دارد.

T23: حذف لاگ‌ها

در صورتی که مجوزهای دسترسی به لاگ‌ها به درستی پیکربندی نشده باشد، امکان حذف عمدی یا غیرعمدی لاگ‌ها برای افراد مجاز و غیرمجاز فراهم می‌شود.

اثر تهدید:

با توجه به اینکه لاگ‌ها در شناسایی فعالیت‌های کاربران و تحلیل علت حوادث، اهمیت دارند، حذف آنها می‌تواند اثرات مخربی همانند مواردی که برای تهدید T21 برشمرده شد، به جای بگذارد.

عاملین تهدید: TA03، TA04، TA06 و TA07

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

راهکار ارائه شده برای تهدید T21 در اینجا نیز مصداق دارد.

T24: ایجاد اختلال برای دسترسی کاربران

هرچند مکانیزم قفل حساب کاربری، امکان اجرای تکنیک‌های Brute Force برای بدست آوردن نامهای کاربری و کلمات عبور معتبر کاربران را کاهش می‌دهد، اما مهاجم ممکن است با سوءاستفاده از همین مکانیزم، حساب‌های کاربری که نام کاربری معتبر آنها را بدست آورده است، به سیستم، قفل کرده و دسترسی آنها را مختل کند. ضمنا با توجه به اینکه از قفل خارج کردن حساب کاربری، به صورت دستی انجام می‌گیرد، تیم پشتیبانی نیز مدام درگیر این موضوع خواهند شد.

اثر تهدید:

این تهدید، منجر به ایجاد اختلال در دسترسی کاربران معتبر سیستم خواهد شد و تیم پشتیبانی نیز درگیر خواهد شد.

عاملین تهدید: TA04

دسته‌بندی STRIDE: Spoofing

راهکار رفع یا کاهش اثر تهدید:

راهکار ارائه شده برای تهدید T08 در اینجا نیز قابل استفاده است.

T25: تنظیم نادرست پالیسی‌های سرویس‌ها

به ازای هر سرویس OpenStack، می‌توان پالیسی‌های کنترل دسترسی به منابع تحت مدیریت آن سرویس را در یک فایل policy.json تعریف کرد. به عنوان مثال APIهای ارائه شده توسط سرویس‌ها، نمونه‌ای از منابعی هستند که قوانین دسترسی به آنها، به کمک این فایلها قابل تنظیم است. با توجه به اینکه این فایل‌ها قابل به‌روزرسانی و ویرایش هستند، ویرایش نادرست آنها می‌تواند منجر به ایجاد نقطه ضعف در سیستم کنترل دسترسی به منابع سرویس شود.

اثر تهدید:

تنظیم نادرست پالیسی‌های کنترل دسترسی به منابع سرویس‌ها، منجر به ایجاد دسترسی غیرمجاز به آن منابع خواهد شد.

عاملین تهدید: TA03

دسته‌بندی STRIDE: Tampering

راهکار رفع یا کاهش اثر تهدید:

بهتر است هر نوع تغییر در فایل‌های policy.json مورد پایش و بررسی قرار گیرد. ضمنا ایجاد تغییرات مجاز و درست در این فایلها باید بلافاصله در سرویس اعمال شود و نیازی به راه‌اندازی مجدد آن سرویس وجود نداشته باشد.

T26: دسترسی بیش از حد ادمین به محتواهای ذخیره شده کاربران

با توجه به اینکه ادمین می‌تواند به محتواهای ذخیره شده تمام کاربران به طور کامل دسترسی داشته باشد، امکان سوءاستفاده از این دسترسی و دستکاری محتواها، حذف آنها به صورت عمد و غیرعمد فراهم خواهد شد.

اثر تهدید:

این تهدید می‌تواند اثرات مختلفی اعم از دستکاری محتواها، حذف آنها و غیره به دنبال داشته باشد.

عاملین تهدید: TA02 و TA03

دسته‌بندی STRIDE: Tampering، Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

بهتر است در اعطای دسترسی‌ها به نقش‌های مختلف، اصل حداقل دسترسی در نظر گرفته شود.

T27: دسترسی غیرمجاز به اطلاعات حساس در پایگاه‌داده‌های موقت

در صورتی که در پایگاه‌داده‌های موقت مورداستفاده سیستم سادا، اطلاعات حساسی همانند توکن‌های دسترسی ذخیره شوند و هیچ نوع احرازهویت روی این حافظه‌ها انجام نشود، و همچنین اطلاعات به صورت plaintext در آن ذخیره شوند، امکان دسترسی غیرمجاز به اطلاعات و افشای آنها وجود خواهد داشت. به عنوان مثال، سیستم Memcached حاوی هیچ مکانیزم داخلی برای احرازهویت نیست و در صورت عدم پیکربندی یک مکانیزم خارجی برای آن، امکان دسترسی به محتواهای ذخیره شده در آن وجود دارد.

اثر تهدید:

در اثر این تهدید، مهاجم می‌تواند به اطلاعات حساس موجود در پایگاه‌داده‌های موقت دست یابد.

عاملین تهدید: TA04

دسته‌بندی STRIDE: Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

بهتر است پیکربندی‌های امنیتی موردنیاز برای حافظه‌های موقت بر طبق best practiceهای موجود انجام شود. به عنوان مثال در این لینک و این لینک نمونه‌ای از این پیکربندی‌ها برای Memcached آورده شده است.

T28: سوءاستفاده از حساب‌های کاربری قدیمی

در صورتی که فهرست کاربران سادا و دسترسی‌های آنها به درستی مستند و مدیریت نشود و مثلا کاربرانی که یک واحد را ترک کرده‌اند، همچنان به این سیستم دسترسی داشته باشند، امکان سوءاستفاده از حساب کاربری آنها توسط مهاجمین داخلی و حتی خود این افراد وجود خواهد داشت. البته مدیریت کاربرانی که از طریق سرور LDAP احرازهویت می‌شوند، برعهده این سرور است اما در صورتی که سمت سادا مدیریتی روی آنها و فعالیتهایشان وجود نداشته باشد، امکان سوءاستفاده از این حساب‌ها فراهم خواهد شد.

اثر تهدید:

با توجه به نقش کاربری که حساب کاربری او مورد سوءاستفاده قرار می‌گیرد، این تهدید می‌تواند اثرات مختلفی داشته باشد. به عنوان مثال، حساب کاربری مدیر ارشد سادا تمام دسترسی‌ها را دارد و انواع پیکربندی‌ها می‌تواند انجام دهد و توانایی ایجاد تاثیرات بسیار مخربی روی سیستم خواهد داشت.

عاملین تهدید: TA04

دسته‌بندی STRIDE: Spoofing

راهکار رفع یا کاهش اثر تهدید:

بهتر است مدیریت کاربران به صورت کامل و دقیق قابل انجام باشد و فعالیت‌های کاربران رصد شود.

T29: افشای اطلاعات حساس و داخلی در خطاها

در صورت عدم مدیریت درست خطاها و پیغام‌های مربوطه، امکان افشای اطلاعات حساس داخلی سیستم به کاربران در پاسخ‌های بازگشتی به آنها وجود خواهد داشت. به عنوان مثال، در صورتی که مقدار پارامتر insecure_debug در فایل پیکربندی Keystone به درستی تنظیم نشده باشد، امکان افشای اطلاعاتی با جزئیات بیشتر فراهم خواهد بود.

اثر تهدید:

مهاجمین همواره به دنبال جمع‌آوری اطلاعات از سیستم مورد هدف خود هستند تا بیشترین شناخت را از قربانی خود بدست آورند و بتوانند در حملات بعدی خود از این اطلاعات استفاده کنند.

عاملین تهدید: TA04

دسته‌بندی STRIDE: Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

بهتر است مقدار پارامتر insecure_debug در فایل پیکربندی Keystone به مقدار false تنظیم شود (لینک راهنما)

T30: دسترسی غیرمجاز به اطلاعات ذخیره شده در ELK

در صورتی که پیکربندی‌های امنیتی در ELK Stack انجام نشده باشد، امکان دسترسی غیرمجاز کاربران به لاگ‌های ذخیره شده در این سیستم فراهم خواهد شد.

اثر تهدید:

این تهدید امکان افشای اطلاعات ذخیره شده در ELK که شامل لاگ‌های سیستم سادا خواهد بود، به دنبال خواهد داشت.

عاملین تهدید: TA05 و TA04

دسته‌بندی STRIDE: Spoofing، Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

پیشگیری از دسترسی غیرمجاز به داده‌ها با تعریف نقش‌ها و تنظیم درست مجوزهای دسترسی آنها، فیلتر کردن IP کلاینت‌ها، عدم استفاده از کلمات عبور پیش‌فرض و ساده، امنسازی ارتباطات با ELK برمبنای TLS و فعال کردن audit logging، نمونه‌ای از پیکربندی‌های امنیتی ELK است. توضیحات بیشتر این پیکربندی‌ها در این لینک، آورده شده است.

T31: شنود ارتباطات بین مولفه‌های مختلف Kafka و دسترسی غیرمجاز به آنها

در صورتی که پیکربندی Kafka انجام نشده باشد، امکان شنود ارتباطات، دسترسی غیرمجاز به داده‌ها وجود خواهد داشت.

اثر تهدید:

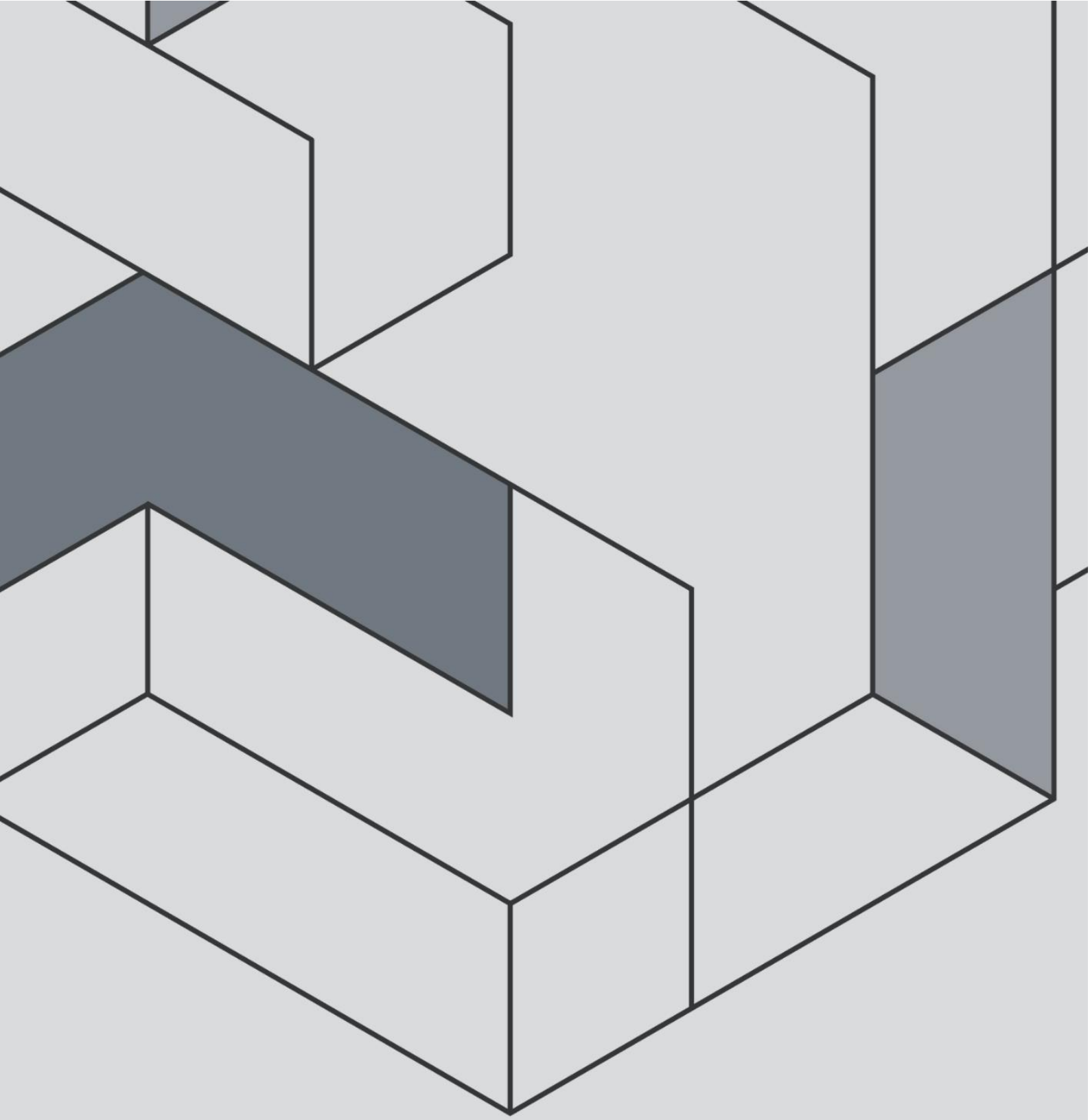
با توجه به اینکه داده‌های رد و بدل شده بین مولفه‌های مختلف Kafka در سیستم سادا شامل لاگ‌های مولفه‌ها و سرویس‌های مختلف این سیستم است، هر نوع دسترسی غیرمجاز به آنها منجر به افشای اطلاعات موجود در لاگ‌ها خواهد شد.

عاملین تهدید: TA04 و TA05

دسته‌بندی STRIDE: Spoofing، Information Disclosure

راهکار رفع یا کاهش اثر تهدید:

رمزنگاری ارتباطات مولفه‌های مختلف Kafka، احرازهویت کلاینت‌ها، فعالسازی و پیکربندی ACLها نمونه‌ای از فعالیت‌هایی هستند که در راستای امنسازی Kafka باید انجام داد. برای کسب اطلاعات بیشتر می‌توان به این لینک مراجعه کرد.



www.aminraay.com
info@aminraay.com
+98 21 44899372
+98 24 33411694